CLAIMS

Sub a1

What is claimed is:

1. A method of providing remote cryptographic services, the method comprising:

a client requesting a cryptographic service;

establishing a secure connection between the client and a biometric certification server (BCS);

receiving biometric data from a user;

the BCS performing the cryptographic service if the user is authenticated based on the biometric authentication; and

the BCS returning the data to the client.

2. The method of claim 1, wherein the cryptographic service is authenticating the user to an other server.

3. The method of claim 2, further comprising the BCS:

generating a temporary public key/private key pair for the user; and

certifying the public key; and

forwarding the certificate to the other server.

4. The method of claim 3, further comprising:

the client receiving data from the other server for signing with the user's private key;

forwarding the data to the BCS; and

the BCS signing the data with the user's temporary private key.

5. The method of claim 4, further comprising:

the client generating a session key for use with the other server, and encrypting the session key with a public key of the other server; and

the client closing the secure connection between the client and the BCS once the session is established between the client and the other server.

6. The method of claim 2, further comprising:

detecting an access to a certification database of the client by an other server;

inserting a temporary certification from the BCS into the certification database of the client; and

generating a true certificate if the other server chooses the temporary certification.

7. The method of claim 1, wherein the cryptographic service is signing or encrypting data.

8. The method of claim 7, further comprising the BCS:

retrieving a private key/public key pair for the user; and

performing the cryptographic service with the private or the public key.

9. The method of claim 1, wherein the client requesting a cryptographic service comprises on of the following: detecting an access to a certificate database of the client, detecting the user attempting to perform a cryptographic activity.

10. A method of providing a certificate from a client to a server, the method comprising:

receiving a request for a certificate from the server;

forwarding the request to a biometric certification server (BCS);

receiving a biometric identification from the client and forwarding the biometric identification to the BCS;

if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS; and

forwarding the certificate to the server, thereby identifying the client to the server.

11. The method of claim 10, further comprising:

detecting an access to a certification database by the server;

inserting a temporary certification from the BCS into the certification database; and

generating a true certificate if the server chooses the temporary certification.

12. The method of claim 10, further comprising:

the BCS generating a disposable public/private key pair in response to the request; and

the BCS certifying the disposable public key of the user.

13. An apparatus for performing remote cryptographic functions comprising:

a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;

an authentication engine for authenticating the user based on biometric data;

a cryptographic engine for performing the cryptographic functions; and

the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

14. The apparatus of claim 13, further comprising:

a database including user credentials;

the authentication engine retrieving user biometric template from the database and comparing the biometric template to the biometric data received from the user.

15. The apparatus of claim 13, further comprising:

a dynamic key generation engine for generating a temporary public key/private key pair, the key pair used for establishing a session between the client and an other server.

16. The apparatus of claim 15, further comprising the cryptographic engine generating a certificate including the temporary public key, certified by the crypto-server's private key.

17. The apparatus of claim 15, the dynamic key generation engine destroying the temporary key pair after the session between the client and the other server is successfully established.

18. The apparatus of claim 13, further comprising:

user self-registration interface permitting a user to chose a handle and register a biometric template.

19. The apparatus of claim 18, further comprising:

a registration engine for receiving biometric data from the user during a registration process, and further for extracting the biometric template for the user; and

a user credential database for storing the handle and the biometric template of the user.

20. The apparatus of claim 17, further comprising:

the registration engine further for generating a persistent private key/public key pair; and

a database for storing the persistent private key/public key pair.

21. The apparatus of claim 13, further comprising:

a database for storing a persistent private key/public key pair; and

the cryptographic engine for using the persistent private key or public key when appropriate to perform the cryptographic functions.

22. An apparatus for permitting remote cryptographic functions comprising:

a crypto-API (application program interface) for receiving cryptographic function requests; and

a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and

a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user.

23. An apparatus comprising:

a client comprising:

a crypto-API (application program interface) for receiving cryptographic function requests; and

a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and

a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user;

the remote crypto-server comprising:

a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection;

an authentication engine for authenticating the user based on the biometric data;

a cryptographic engine for performing the cryptographic functions; and

the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.